Smart TPM

Benutzerhandbuch

Rev. 1001

- Wir empfehlen Ihnen, die neuste Version von Smart TPM von der GIGABYTE-Website herunterzuladen.
- Wenn Ultra TPM bereits früher installiert wurde, können Sie Smart TPM direkt, d. h. ohne vorherige Deinstallation von Ultra TPM, installieren. Die ursprünglichen Einstellungen von Ultra TPM bleiben erhalten.

Inhaltsverzeichnis

TPM-Konfigurationsvorgang 3
1. Das System-BIOS konfigurieren 3
2. Installation des Infineon TPM-Treibers und der Smart TPM-Utility 4
2.1. Installation des Infineon TPM-Treibers 4
2.2. Installation der Smart TPM Utility 4
3. Den TPM-Chip initialisieren 5
3.1. Initialisierung des TPM-Chips mit der Smart TPM-Utility 5
4. Das Hilfsprogramm Smart TPM konfigurieren 8
4.1. Anlegen eines USB-Schlüssels 8
4.2. Anlegen eines Bluetooth-Mobiltelefonschlüssels 9
4.3. Sonstige Bluetooth-Einstellungen 11
4.4. Sonstige Funktionen 11

TPM-Konfigurationsvorgang

Folgen Sie bitte den nachstehenden Schritten, um das TPM zu aktivieren:

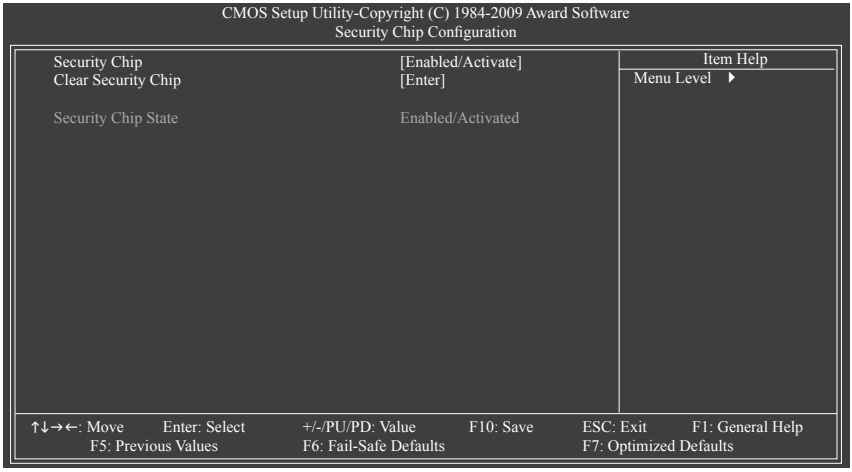
1. Das System-BIOS konfigurieren
2. Installation des Infineon TPM-Treibers und der Smart TPM-Utility
3. Den TPM-Chip initialisieren
4. Konfiguration der Smart TPM-Utility

1. Das System-BIOS konfigurieren

Um die TPM-Funktion zu benutzen, müssen Sie zuerst das System-BIOS aufrufen und dort den TPM-Chip aktivieren.

Schritt 1:
Öffnen Sie das BIOS Setup, wenn der Computer hochfährt. Öffnen Sie das Menü **Security Chip Configuration**. Es erscheint der folgende Bildschirm. Um den TPM-Chip zu aktivieren, setzen Sie **Security Chip** auf **Enabled/Activate**. Es wird empfohlen, die Einstellung **Clear Security Chip** (drücken Sie im BIOS-Hauptmenü auf <Strg> + <F1>, um die Einstellung anzuzeigen) zu verwenden, um den TPM-Chip zu löschen.

Verschlüsselte Dateien können nicht mehr geöffnet werden, wenn der TPM-Chip gelöscht wird. Stellen Sie deshalb sicher, dass die verschlüsselten Dateien zuerst entschlüsselt werden.



Schritt 2:
Wenn Sie alle Einstellungen vorgenommen haben, drücken Sie auf <F10>, um Ihre Änderungen zu speichern und das BIOS Setup zu verlassen.

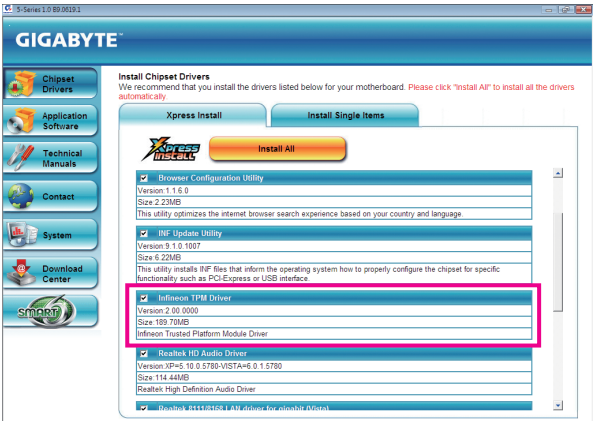
Um zu verhindern, dass andere Benutzer die TPM-Einstellungen löschen, empfehlen wir Ihnen, dass Sie im BIOS Setup ein Benutzerkennwort einrichten.

2. Installation des Infineon TPM-Treibers und der Smart TPM-Utility

Versichern Sie sich vor Verwendung von Smart TPM, dass der Infineon TPM-Treiber und Smart TPM installiert wurden.

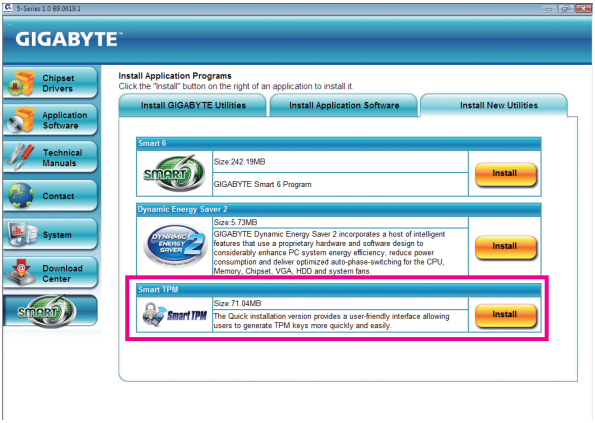
2.1. Installation des Infineon TPM-Treibers

Legen Sie die Treiberdisk für das GIGABYTE-Motherboard ein. "Xpress Install" durchsucht Ihr System automatisch und erstellt eine Liste aller Treiber, deren Installation empfohlen wird. Klicken Sie auf die Schaltfläche **Install All**, um "Xpress Install" alle ausgewählten Treiber, inklusive des Treibers für Infineon TPM, installieren zu lassen.


GIGABYTE
Chipset Drivers
Application Software
Technical Manuals
Contact
System
Download Center
Install Chipset Drivers
We recommend that you install the drivers listed below for your motherboard. Please click "Install All" to install all the drivers automatically.
Xpress Install
Install Single Items
Install All
Browser Configuration Utility
Version:1.1.6.0
Size:2.23MB
This utility optimizes the internet browser search experience based on your country and language.
INF Update Utility
Version:9.1.0.1007
Size:6.22MB
This utility installs INF files that inform the operating system how to properly configure the chipset for specific functionality such as PCI-Express or USB interface.
Infineon TPM Driver
Version:2.00.0000
Size:189.70MB
Infineon Trusted Platform Module Driver
Realtek HD Audio Driver
Version:XP=5.10.0.5780-VISTA=6.0.1.5780
Size:114.44MB
Realtek High Definition Audio Driver

2.2. Installation der Smart TPM Utility

Klicken Sie unten im linken Feld des Autorun-Bildschirms auf die Registerkarte, um das Menü **Install New Utilities** zu öffnen. Klicken Sie zur Installation auf die Schaltfläche **Install** auf der rechten Seite von Smart TPM.


GIGABYTE
Chipset Drivers
Application Software
Technical Manuals
Contact
System
Download Center
Install Application Programs
Click the "Install" button on the right of an application to install it.
Install GIGABYTE Utilities
Install Application Software
Install New Utilities
Smart 6
Size:242.19MB
GIGABYTE Smart 6 Program
Install
Dynamic Energy Saver 2
Size:5.73MB
GIGABYTE Dynamic Energy Saver 2 incorporates a host of intelligent features that use a proprietary hardware and software design to considerably enhance PC system energy efficiency, reduce power consumption and deliver optimized auto-phase-switching for the CPU, Memory, Chipset, VGA, HDD and system fans.
Install
Smart TPM
Size:71.04MB
The Quick installation version provides a user-friendly interface allowing users to generate TPM keys more quickly and easily.
Install

Verschiedene Motherboard-Treiberdisks führen die Smart TPM-Utility in "Xpress Install" aus. Klicken Sie auf die Schaltfläche "Install All" im Hauptmenü von "Xpress Install", um den Infineon TPM-Treiber und Smart TPM zu installieren.

3. Den TPM-Chip initialisieren

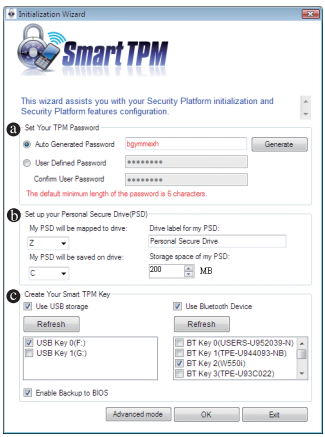
Nach Konfiguration des System-BIOS und Installation der Treiber-Software, erscheint im Meldungsbereich das Infineon Security Platform-Symbol , das Ihnen anzeigt, dass die Infineon Security Platform noch nicht initialisiert wurde. Doppelklicken Sie auf das Symbol oder klicken Sie mit der rechten Maustaste auf das Smart TPM-Symbol und wählen Sie **Initialization Wizard**, um Smart TPM zu öffnen. Smart TPM ermöglicht Ihnen, den TPM-Chip zu initialisieren, ein Benutzerkennwort für TPM einzurichten, ein Personal Secure Drive (PSD) zu konfigurieren und einen mobilen Benutzerschlüssel zu erstellen (siehe Hinweise in Abschnitt 3.1). Durch Auswahl von **Advanced Mode** (siehe Hinweise in Abschnitt 3.2) haben Sie die Möglichkeit, den Initialisierungsassistenten der Infineon Security Platform zu starten und die erweiterten Einstellungen der Infineon Security Platform zu konfigurieren.

3.1. Initialisierung des TPM-Chips mit der Smart TPM-Utility

Die benutzerfreundliche Smart TPM-Oberfläche bietet eine einfache Möglichkeit, um den TPM-Chip zu initialisieren, ein Benutzerkennwort für TPM einzurichten und ein Personal Secure Drive zu konfigurieren.

- **Smart TPM vereinfacht den Konfigurationsvorgang der Infineon Security Platform-Initialisierung und ihrer Funktionen. Für weitere Einstellungen wählen Sie bitte "Advanced Mode".**
- **Smart TPM bietet nur die Einstellung "Datei- und Ordnerverschlüsselung - Personal Secure Drive (PSD)". Um die Funktionen "Sichere E-Mail" oder "Datei- und Ordnerverschlüsselung - Encrypting File System (EFS)" zu verwenden, wählen Sie bitte "Erweiterter Modus".**

3.1.1. Die Smart TPM-Benutzeroberfläche



ⓐ Einstellung Ihres TPM-Kennwortes
Ein Kennwort wird automatisch zugewiesen. Sie können dieses Kennwort in ein eigenes Kennwort ändern. Stellen Sie sicher, dass Sie Ihr Kennwort nicht vergessen; es ermöglicht Ihnen, Ihr Bluetooth-Mobiltelefon oder USB Flash-Laufwerk als mobilen Benutzerschlüssel einzurichten.

ⓑ Einrichtung Ihres Personal Secure Drive (PSD)
Hier konfigurieren Sie ein Personal Secure Drive (PSD). Geben Sie die PSD-Laufwerkskennung an, das Laufwerk-Label, die Größe und ein lokales Laufwerk, auf dem Ihr PSD gespeichert wird.

ⓒ Erstellen Ihres Smart TPM-Schlüssels
Stellen Sie Ihr Bluetooth-Mobiltelefon/USB Flash-Laufwerk als Benutzerschlüssel für Smart TPM ein. Benutzer können ihre PSD-Daten öffnen/schließen, indem sie sich mit dem Bluetooth-Mobiltelefon verbinden oder das USB Flash-Laufwerk, das als Benutzerschlüssel für Smart TPM konfiguriert ist, anstecken.

3.1.2. Initialisierungsvorgang für Smart TPM

Schritt 1: Einstellung Ihres TPM-Benutzerkennwortes

1. Automatisch erstelltes Kennwort

Beim Starten von Smart TPM wird automatisch ein Kennwort zugewiesen. Um ein neues Kennwort zu erzeugen, klicken Sie auf **Generate**.

2. Benutzerdefiniertes Kennwort/Benutzerkennwort bestätigen

Im Feld **User Defined Password** können Sie ein eigenes Kennwort anlegen (max. 16 Zeichen. Geben Sie das Kennwort zur Bestätigung noch einmal in das Feld **Confirm User Password** ein.

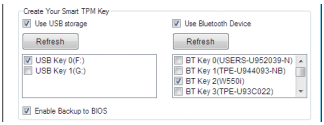
- **Um zu verhindern, dass andere Benutzer die TPM-Einstellungen löschen, empfehlen wir Ihnen, dass Sie im BIOS Setup ein Benutzerkennwort einrichten.**
- **Dieses Kennwort beinhaltet die Funktionen "Besitzerkennwort", "Benutzerkennwort", "Kennwort für Notfall-Wiederherstellungstoken" und "Kennwort für Kennwort-Reset-Token" der Infineon Security Platform. Stellen Sie sicher, dass Sie sich dieses Kennwort für die künftige Verwaltung und Verwendung der Security Platform merken. Einzelheiten zu den Regeln der Infineon Security Platform-Kennwörter und deren Gebrauch finden Sie in der Dokumentation zu Infineon Security Platform.**

Schritt 2: Ein Personal Secure Drive (PSD) einrichten

1. **Geben Sie einen Laufwerkbuchstaben und eine Bezeichnung für Ihr Personal Secure Drive an**
   Um den Laufwerkbuchstaben für Ihr Personal Secure Drive anzugeben, wählen Sie bitte einen unbenutzten Buchstaben aus der Dropdown-Liste unter **My PSD will be mapped to drive** aus.Um die Laufwerkbezeichnung anzugeben, geben Sie die Bezeichnung in das Feld unter **Drive label for my PSD** ein. Die Bezeichnung darf maximal 32 Zeichen haben.
2. **Geben Sie die Größe des Personal Secure Drive und ein lokales Laufwerk, in dem das Personal Secure Drive gespeichert werden soll, an**
   Wählen Sie ein lokales Laufwerk aus der Dropdown-Liste unter **My PSD will be saved on drive]** aus und geben die Größe des Personal Secure Drive in dem Feld **Storage space of my PSD** an.

Die Größe des Personal Secure Drive kann nicht nach dem Einstellen geändert werden. Achten Sie deshalb bitte darauf, dass die angegebene Größe für Ihre Bedürfnisse ausreicht.Nehmen Sie bitte zur Kenntnis, dass Sie die Größe des Laufwerks nicht ausnützen können, da das Dateisystem einigen Platz belegt.Die Größe des belegten Speicherplatzes hängt von dem Betriebssystem ab und kann im Fall einer kleinen Laufwerkgröße erheblich auffallen.Nehmen Sie bitte auch zur Kenntnis, dass die Größe des PSD eine Obergrenze hat:
Die Größe des PSD in einem FAT16-Laufwerk darf maximal 2 GB sein.
Die Größe des PSD in einem FAT32-Laufwerk darf maximal 4 GB sein.

Schritt 3: Erstellen Ihres Smart TPM-Schlüssels

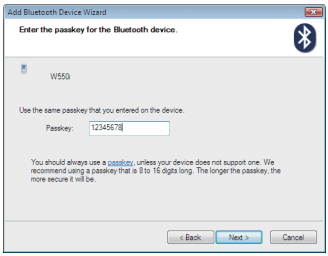


1. Anlegen eines USB-Schlüssels:

Markieren Sie das Kontrollkästchen **Use USB storage** und klicken Sie auf **Refresh**, um nach angeschlossenen USB Flash-Laufwerken zu suchen. Wählen Sie dann das USB Flash-Laufwerk aus, das Sie als mobilen Smart TPM-Benutzerschlüssel verwenden möchten. Sie können mehr als ein USB Flash-Laufwerk auswählen. Durch Auswahl von **Enable Backup to BIOS** wird das verschlüsselte TPM-Benutzerkennwort im System-BIOS hinterlegt.

Werden mehrere verschlüsselte TPM-Benutzerkennwörter im BIOS gespeichert, überschreibt das neue Kennwort das alte.

2. Anlegen eines Bluetooth-Mobiltelefonschlüssels:


Add Bluetooth Device Wizard
Enter the passkey for the Bluetooth device.
W550i
Use the same passkey that you entered on the device.
Passkey:
12345678
You should always use a passkey, unless your device does not support one. We recommend using a passkey that is 8 to 16 digits long. The longer the passkey, the more secure it will be.
< Back
Next >
Cancel

Markieren Sie das Kontrollkästchen Use **Bluetooth Device** und klicken Sie auf **Refresh**, um nach Bluetooth-Mobiltelefonen zu suchen. Wählen Sie anschließend das Mobiltelefon aus, das Sie als mobilen Smart TPM-Benutzerschlüssel verwenden möchten. Daraufhin erscheint ein Bildschirm ähnlich dem links gezeigten. Geben Sie unter **Passkey** einen Kenncode (empfohlen sind 8~16 Zeichen) für die Paarung mit Ihrem Mobiltelefon ein. Geben Sie dann für die Paarung den gleichen Kenncode an Ihrem Mobiltelefon ein.

Versichern Sie sich vor Erstellung eines Bluetooth-Mobiltelefonschlüssels, ob Ihr Motherboard einen Bluetooth-Empfänger enthält und schalten Sie die Suche und die Bluetooth-Funktionen an Ihrem Mobiltelefon ein.

Wenn Sie die oben aufgeführten Schritte durchgeführt haben, klicken Sie auf **OK**, um die Initialisierung des TPM-Chips zu beginnen und das TPM-Benutzerkennwort, Ihre PSD und den oder die Smart TPM-Benutzerschlüssel einzurichten.

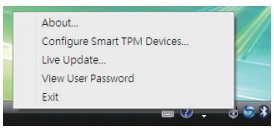
4. Das Hilfsprogramm Smart TPM konfigurieren

Das einzigartige Smart TPM (Trusted Platform Module) von GIGABYTE unterstützt die modernsten hardwarebasierten Datenverschlüsselungstechniken. Smart TPM bietet eine benutzerfreundliche Software-Oberfläche, um mit einem Bluetooth-Mobiltelefon oder einem USB Flash-Laufwerk mobile Benutzerschlüssel zu erstellen. Benutzer können ihre PSD-Daten öffnen/schließen, indem sie sich mit dem Bluetooth-Mobiltelefon verbinden oder das USB Flash-Laufwerk, das als Benutzerschlüssel für Smart TPM konfiguriert ist, anstecken - ganz ohne umständliche Konfiguration. Zudem kann mehr als ein Bluetooth-Mobiltelefon/USB Flash-Laufwerk als Schlüssel eingestellt werden, damit Sie bei einem etwaigen Verlust des Schlüssels weiterhin auf Ihre Daten zugreifen können.

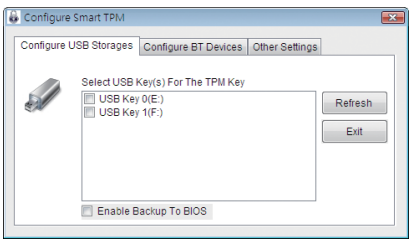
- **Wenn Sie Ihre Kennwörter und Schlüssel für TPM erstellt haben, sorgen Sie dafür, dass Sie diese an einem sicheren Ort aufbewahren und sichern. Bei einem Verlust der Kennwörter und/oder Schlüssel können verschlüsselte Daten nicht mehr geöffnet oder gelesen werden.**
- **Obwohl TPM die neuste Datensicherheitstechnik zur Verfügung stellt, wird keine Datenintegrität garantiert und es wird kein Hardwareschutz geboten. GIGABYTE haftet nicht für den Verlust von verschlüsselten Daten durch Hardwareschäden.**

4.1. Anlegen eines USB-Schlüssels

Schritt 1:
Nach Initialisierung des TPM-Chips und Einrichtung des Benutzerkennwortes für TPM sowie Ihrer PSD klicken Sie mit der rechten Maustaste auf das Smart TPM-Symbol im Meldungsbereich, um das unten gezeigte Menü zu öffnen.

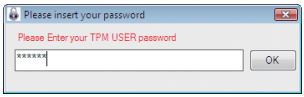


Schritt 2:
Klicken Sie auf **Configure Smart TPM Devices**, um die Smart TPM-Utility zu starten. Um einen mobilen USB-Schlüssel zu erstellen, wählen Sie **Configure USB Storages** und dann das USB Flash-Laufwerk, das Sie als mobilen Benutzerschlüssel verwenden möchten. (wenn das angeschlossene USB Flash-Laufwerk nicht angezeigt wird, klicken Sie auf **Refresh**, um das Gerät von Smart TPM erkennen zu lassen).



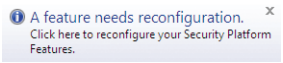
Wenn mehrere Benutzer die Funktion "Sicherung im BIOS" verwenden, um ihre verschlüsselten TPM-Benutzerkennwörter im BIOS zu speichern, überschreibt das neue Kennwort das alte.

Schritt 3:
Geben Sie das zuvor eingestellte TPM-Benutzerkennwort ein und klicken Sie auf **OK**, um die Erstellung des USB-Schlüssels abzuschließen. Jetzt können Sie Ihre PSD öffnen/schließen, indem Sie das USB Flash-Laufwerk anstecken oder trennen.

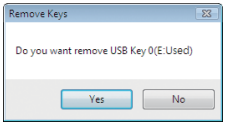


Während der USB-Schlüssel erstellt wird, darf der Computer nicht abgeschaltet oder zurückgesetzt werden.

- **Wenn das TPM-Benutzerkennwort drei Mal falsch eingegeben wird, wird Smart TPM gesperrt. Der Computer darf weder ausgeschaltet noch neu gestartet werden, wenn ein Benutzerschlüssel generiert wird.**
- **Das Infineon Security Platform-Einstellungstool gibt folgende Warnung aus, wenn der USB-Schlüssel abgesteckt wird.**

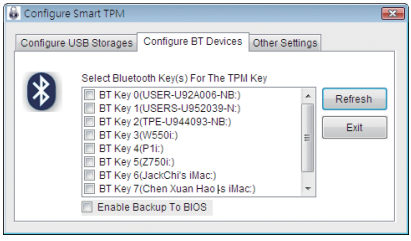


Widerrufen eines USB-Schlüssels:
Um einen USB-Schlüssel zu widerrufen, entfernen Sie auf der Registerkarte **Configure USB Storages** die Markierung von dem USB Flash-Laufwerk, das als Smart TPM-Benutzerschlüssel konfiguriert ist . Bestätigen Sie mit **Yes**. Der USB-Schlüssel wird daraufhin widerrufen.



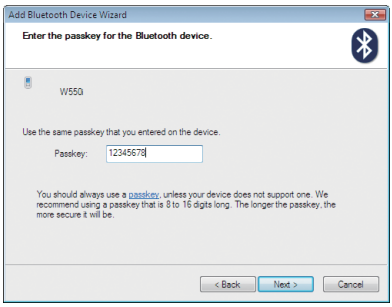
4.2. Anlegen eines Bluetooth-Mobiltelefonschlüssels

Schritt 1:
Um einen mobilen Bluetooth-Mobiltelefonschlüssel zu erstellen, wählen Sie **Configure BT Devices** und dann das Bluetooth-Mobiltelefon, das Sie als mobilen Benutzerschlüssel verwenden möchten. (wenn das Bluetooth-Mobiltelefon nicht angezeigt wird, klicken Sie auf **Refresh**, um das Gerät von Smart TPM erkennen zu lassen).

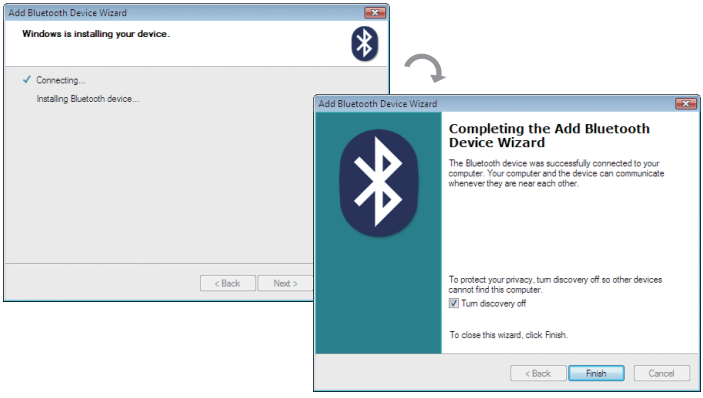


Versichern Sie sich vor Erstellung eines Bluetooth-Mobiltelefonschlüssels, ob Ihr Motherboard einen Bluetooth-Empfänger enthält und schalten Sie die Suche und die Bluetooth-Funktionen an Ihrem Mobiltelefon ein.

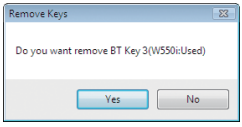
Schritt 2:
Wenn der **Add Bluetooth Device Wizard** erscheint, geben Sie einen Kenncode für die Paarung mit Ihrem Mobiltelefon ein (empfohlen sind 8~16 Zeichen).


Add Bluetooth Device Wizard
Enter the passkey for the Bluetooth device.
W550i
Use the same passkey that you entered on the device.
Passkey:
12345678
You should always use a passkey, unless your device does not support one. We recommend using a passkey that is 8 to 16 digits long. The longer the passkey, the more secure it will be.
< Back
Next >
Cancel

Schritt 3:
Geben Sie für die Paarung den gleichen Kenncode an Ihrem Mobiltelefon ein. Nach Bestätigung des Kenncodes klicken Sie auf **Finish** , um die Erstellung des Bluetooth-Mobiltelefonschlüssels abzuschließen. Jetzt können Sie Ihre PSD öffnen/schließen, indem Sie Bluetooth an Ihrem Mobiltelefon ein- oder ausschalten oder wenn Sie sich mit Ihrem Mobiltelefon dem Computer nähern oder von ihm entfernen.


Add Bluetooth Device Wizard
Windows is installing your device.
Connecting...
Installing Bluetooth device...
< Back
Next >
Add Bluetooth Device Wizard
Completing the Add Bluetooth Device Wizard
The Bluetooth device was successfully connected to your computer. Your computer and the device can communicate whenever they are near each other.
To protect your privacy, turn discovery off so other devices cannot find this computer.
Turn discovery off
To close this wizard, click Finish.
< Back
Finish
Cancel

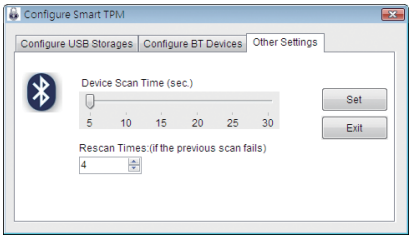
Widerrufen eines Bluetooth-Mobiltelefonschlüssels:
Um einen Bluetooth-Mobiltelefonschlüssel zu widerrufen, entfernen Sie auf der Registerkarte **Configure BT Devices** die Markierung von dem Bluetooth-Mobiltelefon, das als Smart TPM-Benutzerschlüssel konfiguriert ist . Bestätigen Sie mit **Yes**. Der Bluetooth-Mobiltelefonschlüssel wird daraufhin widerrufen.



4.3. Sonstige Bluetooth-Einstellungen

Auf der Registerkarte **Other Settings** können Sie angeben, wie lange der Bluetooth-Mobiltelefonschlüssel gesucht und wie oft die Suche wiederholt werden soll, um zu überprüfen, ob sich das Mobiltelefon in Reichweite des Computers befindet.

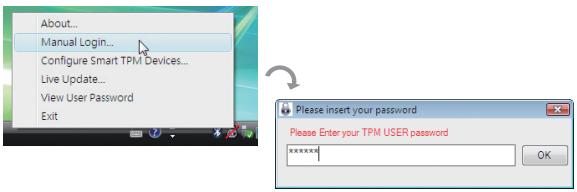
- Geräte Suchzeit (s):
  Stellen Sie ein, wie lange Smart TPM Ihren Bluetooth-Mobiltelefonschlüssel sucht (Einstellbereich: 5 bis 30 Sekunden, in Schritten zu 5 Sekunden). Smart TPM sucht so lange nach Ihrem Schlüssel, wie Sie angeben.
- Suche wiederholen:
  Stellen Sie ein, wie oft Smart TPM die Suche nach Ihrem Bluetooth-Mobiltelefonschlüssel wiederholt, wenn der Schlüssel nicht gefunden wird (Einstellbereich: 1 bis 10 Mal). Smart TPM wiederholt die Suche so oft, wie Sie angeben. Wenn Smart TPM Ihren Bluetooth-Mobiltelefonschlüssel innerhalb der vorgegebenen Zeitbeschränkung nicht gefunden hat, wird die TPM-Funktion abgeschaltet.



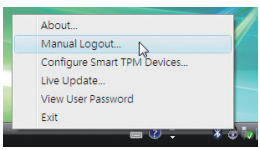
4.4. Sonstige Funktionen

A. Manuelles An-/Abmelden

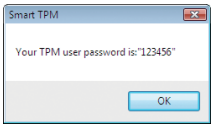
Sie können TPM auch dann aktivieren, wenn Sie Ihren Benutzerschlüssel nicht parat haben. Klicken Sie mit der rechten Maustaste auf das Smart TPM-Symbol im Meldungsbereich und wählen Sie **Manual Login**. Geben Sie das TPM-Benutzerkennwort ein, wenn Sie dazu aufgefordert werden, um TPM zu aktivieren.



Um TPM zu deaktivieren wählen Sie **Manual Logout**.



B. Anzeigen des Benutzerkennwortes



Wählen Sie **View User Password**, um sich das TPM-Benutzerkennwort anzeigen zu lassen.

Diese Funktion setzt voraus, dass Sie Ihren USB-Schlüssel angesteckt oder Bluetooth an Ihrem Bluetooth-Mobiltelefonschlüssel aktiviert haben.